METHOD FOR EFFICIENT COMPUTATION OF POINT DOUBLING OPERATION OF ELLIPTIC CURVE POINT SCALAR MULTIPLICATION OVER FINITE FIELDS F(2M)

ABSTRACT OF THE DISCLOSURE

The present invention provides a method for performing a point doubling operation with only one modular division and no multiply per operation. As a result, the invention reduces the number of mathematical operations needed to perform point doubling operations in elliptic curve computation. An elliptic curve cryptosystem using the present invention can be made to operate more efficiently using the present invention. An elliptic curve crypto-accelerator can be implemented using the present invention to dramatically enhance the performance of the elliptic curve cryptosystem. The invention derives the slope of a curve independently of the y-coordinate. By avoiding the calculation of the y term, one additional multiply is eliminated from each point-doubling operation. Using the invention, n consecutive point doublings can be reduced to n modular divisions and 1 multiply. This avoids the 2n multiplies of prior art approaches.